UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	)	
	)	
v.	)	No. 1:21-cr-00041-JL
	)	
IAN FREEMAN, ET AL	)	
	)	

GOVERNMENT'S OBJECTION TO DEFENDANT'S DAUBERT CHALLENGE TO FORENSIC BLOCKCHAIN ANALYSIS

The defendant does not dispute that the bitcoin blockchain is an authoritative public ledger of every bitcoin transaction that has ever occurred. *United States v. Gratowski*, 964 F.3d 307, 312 (5th Cir. 2020) ("[E]ach bitcoin transaction is recorded in a publicly available blockchain [and e]very bitcoin user has access to the public bitcoin blockchain and can see every bitcoin address and its respective transfers."). The tracing of transactions on this public blockchain, therefore, is akin to a financial analyst tracing money in bank accounts, which would not be the subject of expert testimony. In this case, the government's proposed witness combined such tracing with a basic heuristic commonly relied upon in analyzing virtual currency transactions. This heuristic, known as "co-spend analysis," allowed analysts to determine that certain bitcoin addresses were controlled by the same person. The method relied upon in this case is a fundamental of blockchain analytics. It is well tested, commonly relied upon, replicable using publicly available tools, and corroborated by other aspects of this investigation.

The Defendant's Motion & Procedural Posture

On July 29, 2022, Defendant Aria DiMezzo filed a motion *in limine* to exclude forensic blockchain analysis from the trial. Defendant Freeman joined the motion. The motion primarily

challenged the use of commercial blockchain analytics tools, based on a mistaken assumption that the government intended to rely on those tools at trial.[1] After reviewing the motion, government counsel clarified that it did not intend to rely on those tools at trial, and explained that it was instead focusing on the proposed expert's own application of co-spend analysis to the publicly available blockchain.[2] In order to determine whether defendants would proceed with the motion in light of this information, government counsel offered to allow defendants' counsel to conduct an interview of the proposed expert witness, Erin Montgomery, who serves as a Supervisory Intelligence Analyst with the Federal Bureau of Investigation. The government understood that defendant DiMezzo's counsel, who was handling the issue, intended to question Ms. Montgomery about her use of co-spend analysis and thereafter decide whether to pursue the motion on that basis. Shortly before that interview was to occur, defendant DiMezzo pleaded guilty.

Government counsel provided Ian Freeman's counsel with the same opportunity. Freeman's counsel questioned Ms. Montgomery about her qualifications but did not ask any questions about her use of co-spend analysis. The defendant's counsel then stated that he intended to go forward with the hearing. Given that the written motion challenges the use of commercial tools which will not form the basis for the expert's testimony in this case, the government is not entirely clear about on what basis the defendant intends to challenge Ms. Montgomery's testimony. This response, nevertheless, will describe the proposed testimony and

[1] The defendant's motion states, "although it is not entirely clear, it appears that in this case the Government's agent and designated expert witness may have used commercially available blockchain analysis tools." ECF No. 180 at 4-5. Although the witness did use commercial tools in her investigation, she replicated the results by doing her own analysis of the blockchain using open source tools and her trial testimony will focus only on this work.

[2] The witness used blockchain.com and other websites which facilitate searches of the public bitcoin blockchain.

methodologies used by the witness, and focus on what appears to be the only possible challenge to the witness's testimony, her use of co-spend analysis.

The *Daubert* Standard

Rule 702 of the Federal Rules of Evidence governs the admissibility of expert testimony and lists the four criteria that must to be met to admit expert testimony: 1) the expert's specialized knowledge will help the trier of fact to understand the evidence or determine a fact in issue; 2) the testimony is based on sufficient facts or data; 3) the testimony is the product of reliable principles and methods; and 4) the expert reliably applied the principles and methods to the facts of the case. Fed. R. Evid. 702. Rule 702 was amended in response to *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), and its progeny.

In *Daubert*, the Supreme Court provided several non-exclusive, non-dispositive factors for trial courts to consider when assessing the reliability of expert testimony. These factors include whether an expert's "technique or theory" 1) can be or has been tested; 2) has been subject to peer review and publication; 3) has a known or potential error rate; 4) has maintained operational standards and controls; and 5) has general acceptance in a relevant scientific community. *Id.* at 593-94. Since *Daubert*, the Court has held that district courts are granted "considerable leeway" in determining how to assess reliability, *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 152 (1999), and similarly "broad latitude" for ultimate reliability determinations. *Id.* at 142.

Trial courts perform a gatekeeping function which entails a preliminary evaluation of the proffered expert testimony for both reliability and relevance. *United States v. Diaz*, 300 F.3d 66,

73 (1st Cir. 2002). The Rule 702 inquiry is flexible, with no particular procedure that a trial court must follow in executing that function. *Id.*

The Proposed Testimony

Ms. Montgomery will testify that she analyzed the bitcoin blockchain and identified three clusters of addresses, or "wallets," that were controlled by Ian Freeman. A bit of undisputed background is necessary to understand her methodology:

> Bitcoin is a type of virtual currency. Each Bitcoin user has at least one "address," similar to a bank account number, that is a long string of letters and numbers. Bitcoin users send Bitcoin to other users through these addresses using a private key function that authorizes the payments. To conduct Bitcoin transactions, Bitcoin users must either download Bitcoin's specialized software or use a virtual currency exchange. . . .When a Bitcoin user transfers Bitcoin to another address, the sender transmits a transaction announcement on Bitcoin's public network, known as a blockchain. The Bitcoin blockchain contains only the sender's address, the receiver's address, and the amount of Bitcoin transferred. The owners of the addresses are anonymous on the Bitcoin blockchain, but it is possible to discover the owner of a Bitcoin address by analyzing the blockchain. For example, when an organization creates multiple Bitcoin addresses, it will often combine its Bitcoin addresses into a separate, central Bitcoin address (i.e., a "cluster"). It is possible to identify a "cluster" of Bitcoin addresses held by one organization by analyzing the Bitcoin blockchain's transaction history. Open source tools and private software products can be used to analyze a transaction.

Gratowski, 964 F.3d at 309.

In this case, Ms. Montgomery identified clusters of addresses termed "wallets" that she will testify were controlled by defendant Freeman. The "clustering" heuristic that she relied upon to come to this conclusion is called "co-spend," "shared spend," "common input," "multiple input," or "multi-input" analysis. Co-spending occurs when multiple input addresses are used to send bitcoin in a single transaction, indicating that a single owner holds the private keys for all of those addresses. For example, Person A may control two addresses, one with two bitcoins, and one with three bitcoins. If Person A chose to send Person B five bitcoins, an analysis of the

blockchain would show that the two addresses (holding two and three bitcoins respectively) would have spent bitcoin in the same transaction to transfer five bitcoins to a third address, demonstrating that Person A controlled both the address with two bitcoins and the address with three bitcoins. The concept of co-spend or multi-input analysis is so fundamental that it was discussed in the foundational white paper on bitcoin authored by its inventor. *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 6 (2008) ("Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.")

Ms. Montgomery used this principle to analyze the bitcoin blockchain to determine that a total of 406 addresses were linked in one cluster, dubbed by investigators as the "holding wallet." Ms. Montgomery will also opine, based on review of evidence in the case, that this wallet was controlled by Ian Freeman. She will base this opinion on the fact that various virtual asset service provider ("VASP" or exchange) accounts in Ian Freeman's name sent money to the holding wallet, that the holding wallet was used to send bitcoin to an undercover officer who purchased bitcoin from Ian Freeman, and that it sent bitcoin to another wallet used to fund Mr. Freeman's bitcoin ATMs, among other facts. This part of Ms. Montgomery's conclusion is illustrated in a chart she created, attached as Government's Exhibit 1.[3]

Relevance of the Testimony

As Government's Exhibit 1 shows, the "holding wallet" was funded by exchange accounts opened in the names of Ian Freeman and his co-conspirators, material to the conspiracy

[3] The fact that this wallet has so many independent links to Ian Freeman also corroborates Ms. Montgomery's use of co-spend analysis to link these addresses together.

charge. In addition, the analysis shows that Ian Freeman's addresses funded sales to the undercover agent, the bitcoin ATMs, and other identified bitcoin purchasers. The total amount of funds flowing through his addresses is also relevant to help understand the scope of the business.

Erin Montgomery's Qualifications

Ms. Montgomery is a supervisory intelligence analyst with the FBI, where she has been employed for 14 years. She currently supervises the group at the FBI dedicated to virtual currency intelligence within the Threat Finance and Economic Intelligence Unit. Ms. Montgomery has been involved in bitcoin investigations since 2011 and has extensive experience working on investigations of criminal exploitation of virtual currency. After gaining experience working on many of the FBI's major bitcoin-related investigations, she was tasked with developing the FBI's training program on blockchain investigation and analysis. She has trained thousands of people on these issues.

Reliability of Co-Spend Analysis

As defendant DiMezzo's motion recognizes, "co-spend analysis is the most-used metric in commercial blockchain analysis tools . . . [and is a] foundational element[] of forensic blockchain analysis." ECF No. 180 at 4 (citing Sarah Meiklejohn, *The Limits of Anonymity in Bitcoin,* ROUTLEDGE HANDBOOK OF CRIMINAL SCIENCE (Richard Wortley et al., eds., 2018) at 285). Most published case law on this issue addresses challenges to investigators' reliance on commercial blockchain analytic tools. These tools rely on co-spend analysis among other heuristics to draw conclusions about activity on the blockchain. Although the use of those tools presents more complex issues than reliance solely on the one widely-accepted heuristic of co-

spend analysis, the published cases support their reliability. Those cases are therefore strong support for the acceptance and reliability of the much simpler metric at issue in this case.

Though the government is not aware of courts that have considered a *Daubert* challenge on this issue, testimony about blockchain analytics has frequently been admitted in federal court, sometimes as expert testimony. *See, e.g.*, *United States v. Ologeanu et al*, 5:19-cr-00010 (E.D. Ky.) (defendant Iossifov was convicted at trial following testimony regarding blockchain analysis; multiple other defendants pleaded guilty in advance of trial); *United States v. Dove*, 8:19-cr-33 (M.D. Fla.) (defendant pleaded guilty mid-trial following testimony regarding blockchain analysis); *United States v. Felton*, No. 20-cr-347 (N.D. Ga.) (defendant pleaded guilty mid-trial to multiple counts of wire fraud, securities fraud, and money laundering, following blockchain analysis expert testimony); *United States v. Ulbricht*, 14-cr-68 (S.D.N.Y.) (administrator of Silk Road darknet market convicted at trial that included blockchain analysis testimony) (upheld in *United States v. Ulbricht*, 858 F.3d 71 (2d Cir. 2017)); *United States v. Costanzo*, No. 2:17-cr-00585 (D. Ariz.) (defendant found guilty of money laundering at trial following testimony regarding blockchain analysis) (upheld in *United States v. Costanzo*, 956 F.3d 1088 (9th Cir. 2020). This analysis has also been used in hundreds of other successful criminal investigations and prosecutions.

Courts have also considered the use of blockchain analytic tools in various other contexts, and consistently found them to be reliable. A judge considering a civil forfeiture action in the District of Columbia observed:

> Despite Bitcoin's pseudonymous nature, law enforcement can sometimes identify parties to a transaction. By analyzing the blockchain (the public ledger that records transactions) law enforcement can ascertain the counterparties' unique bitcoin addresses. And because users often combine multiple bitcoin addresses and use them together in the same transaction . . . analysis of one transaction might reveal many addresses belonging to a single individual or organization. Several private

> companies have used that kind of analysis to identify bitcoin address clusters associated with the same parties. With the right clues, one can then attribute a cluster to a particular individual or organization. Authorities took advantage of third-party blockchain software to perform the investigation here.

United States v. 155 Virtual Currency Assets, Civil Action No. 20-cv-2228 (RC), 2021 WL 1340971, at *2. D.D.C. Apr. 9, 2021) (cleaned up).

Blockchain analysis has been considered by judges in issuing search and seizure warrants. The Fifth Circuit considered blockchain analysis in another context in *Gratkowski*, 964 F.3d at 309, after the defendant challenged a warrant based on blockchain analysis tying him to a darknet site trafficking in child sexual abuse materials. The court rejected the defendant's argument that "federal agents' method of using a 'powerful and sophisticated software' to analyze the Bitcoin blockchain intruded into a constitutionally protected area and violated the Fourth Amendment." 964 F.3d at 312 N. 12. The Fifth Circuit observed, "Every Bitcoin user has access to the public Bitcoin blockchain and can see every Bitcoin address and its respective transfers. Due to this publicity, it is possible to determine the identities of Bitcoin address owners by analyzing the blockchain." 964 F.3d at 312. *See also In the Matter of Search of Multiple Email Accts. Pursuant to 18 U.S.C. § 2703 for Investigation of Violation of 18 U.S.C. § 1956,* 2022 WL 406410, at *13 (D.D.C. Feb. 8, 2022) ("The unprecedented rate of prior success, lack of incentive or capacity to lie, and incredible level of detail (the software draws out each transaction block-by-block that comprises a cluster), make the clustering software a reliable foundation for probable cause that is beyond compare").

The use of blockchain analysis software is not limited to criminal investigations. Many major financial institutions use blockchain analysis software tools as part of their anti-money laundering programs needed to comply with their regulatory obligations and monitor their transactions for suspicious activity. *See, e.g.*, New York Department of Financial Services,

Guidance on Use of Blockchain Analysis, April 28, 2022, available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220428_guidance_use_blockchain_analytics (emphasizing "the importance of blockchain analytics" to all virtual currency businesses regulated in New York, including to address anti-money laundering requirements). Blockchain analysis is also used by other government agencies in their matters. *See, e.g.*, U.S. Department of Treasury, *Treasury Takes Robust Actions to Counter Ransomware,* Sept. 21, 2021, https://home.treasury.gov/news/press-releases/jy0364 (announcing designation of Russian cryptocurrency exchange Suex, finding that, "analysis of known SUEX transactions shows that over 40% of SUEX's known transaction history is associated with illicit actors."); *In the Matter of Larry Dean Harmon d/b/a Helix*, 2020-2, Assessment of Civil Money Penalty, available at https://www.fincen.gov/sites/default/files/enforcement_action/2020-10-19/HarmonHelix%20Assessment%20and%20SoF_508_101920.pdf (assessing a civil money penalty against the operator of a darknet mixer after tracing transactions between the mixer and numerous darknet markets and observing that "transactions equal to $121,511,877 transferred to darknet-associated addresses by, through, or to Helix."). Blockchain analysis thus enjoys broad acceptance across a range of industries.

Defendant's characterization of the scholarly literature addressing blockchain analytics does not accurately reflect the modern recognition of co-spend analysis as a core methodology to analyze blockchain transactions. Defendant relies heavily on a 2016 journal article by Luu and Imwinkelried, which considered what at that time was a relatively new methodology under a *Daubert* analysis. Jason Luu and Edward Imwinkelried, *The Challenge of Bitcoin Pseudo-Anonymity to Computer Forensics*, 52 CRIM. L. BULL. 191 (2016). Luu and Imwinkelried based their opinion that blockchain analytics would not pass muster under *Daubert* in large part on the

fact that it was not yet generally accepted, which they admitted was "largely due to the relative novelty of these techniques." *Id.* at 17. Given that the first cited clustering analysis occurred in 2011, it was still relatively novel in 2016, yet much has changed since that time. Further, the article discusses various types of blockchain analytic heuristics and the specific discussion of co-spend analysis is in fact quite favorable. *Id.* at 18. ("[T]here is a stronger case for the admission of testimony based on transaction graph analysis," which includes co-spend analysis). The early studies of blockchain analytics they cited favorably reported on the use of co-spend analysis. *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, PROC. CONF. INTERNET MEAS. CONF. (IMC), 2013, pp. 127–140.

More recent scholarly work on blockchain analytics recognizes the reliability of this very foundational and widely-used method.[4] *See e.g.,* George Kappos et al., *How to Peel a Million: Validating and Expanding Bitcoin Clusters*, 1 (2022), https://arxiv.org/pdf/2205.13882.pdf ("[O]ne heuristic that has been particularly widely adopted is the so-called co-spend heuristic, which says that all addresses used as input to the same transaction belong to the same entity."); Haroon M. Yousef, *Investigating Transactions in Cryptocurrencies* , 29 (Mar. 29, 2022), https://arxiv.org/pdf/2203.14684.pdf (doctoral thesis describing co-spend as the "foundational process used to cluster Bitcoin addresses . . . [t]he effectiveness [of which] has been demonstrated by many researchers."); Yuhang Zhang et al., *Heuristic-Based Address Clustering in Bitcoin*, 8 IEEE Access, 210582, 210582-90 (2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9265226 (describing the multiple-

[4] One exception to the assumption underling the heuristic that all inputs to a transaction are controlled by the same entity is called Coinjoin, "where users work together to create a transaction in which they each control a different input and the outputs likewise represent different recipiences. This acts to mix together the coins of these users." Kappos et al., at 3. Ms. Montgomery will testify that this technique is distinguishable on the blockchain from the transactions she relied upon to link the accounts used by the defendant.

input heuristic as "widely used," and "very effective in clustering addresses that belong to the same user" and noting that, "the multiple input addresses heuristic applies to the greatest number of transactions and is very reliable before the introduction of services such as CoinJoin . . . ."); Martin Harrigan & Christopher Fretter, *The Unreasonable Effectiveness of Address Clustering* 6 (2018), ("New key pairs are not being generated for every transaction allowing the multi-input heuristic to link addresses to a common owner. This is one reason that address clustering is unreasonably effective").

Conclusion

The co-spend analysis relied upon by Ms. Montgomery to conclude that Ian Freeman controlled a cluster of addresses is a foundational element of blockchain analytics, a field which is now generally accepted, has been tested, and is frequently relied upon by courts in various contexts. Ms. Montgomery, who developed the FBI's training curriculum on these issues, is immensely qualified to apply the co-spend methodology. Her analysis is reliable and relevant to the issues at trial.

Respectfully submitted,
JANE E. YOUNG
United States Attorney

Dated: October 26, 2022

/s/ Georgiana L. MacDonald
Assistant U.S. Attorney
MA Bar # 685375
53 Pleasant Street, 4th Floor
Concord, New Hampshire 03301
603-225-1552
georgiana.macdonald@usdoj.gov

/s/ John J. Kennedy

Assistant U.S. Attorney
NH Bar # 19557
53 Pleasant Street, 4th Floor
Concord, New Hampshire 03301
603-225-1552
john.kennedy2@usdoj.gov

/s/ Seth R. Aframe

Assistant U.S. Attorney
53 Pleasant Street, 4th Floor
Concord, New Hampshire 03301
603-225-1552